NIST Cloud Computing Security Workgroup (NCC-SWG) Kick off Meeting Minutes

Time: 2/9/2011 2:00-3:00 PM EST

Online at http://webconf.soaphub.org/conf/room/cc_security

Threads of discussions

1. Mouli@NIST (the host) outlined meeting agenda, and provided his email mouli@nist.gov for correspondence and signup NCC-SWG
2. Mouli@NIST (the host) reviewed NCC-SWG Charter (Draft Version)
3. Discussion about top 5 to 10 issues/priority items that should be addressed by the NCC-WSG. Below are a list of candidates via chat room and phones
   a. Come up with threat taxonomy
   b. Define high level security architecture
   c. Identity federation, standards for interchange of authorization and authentication credentials, federal use cases for identity management
   d. Potential loss of control/ownership of data
   e. Data Integration , Privacy (PII) and Data Encryption
   f. Ability to completely delete / destroy data
   g. Audit Data Integrity protection
   h. Compliances, A&A (C&A)
   i. Virtualization standards and related threats
4. Discussion about NCC-SWG approach
   a. Come up with Threat Taxonomy
   b. Top down approach, define high level security architecture, starting from security core of availability, confidentiality, integrity
   c. NCC-SWG focuses more on security responsibility between CC provider and subscribers, will need high level Reference Architecture (RA) to facilitate it
   d. Activities should be in parallel, NCC-SWG effort cannot wait on Taxonomy WG and RA WG

   e. Leverage existing initiatives and effort such as work done by Cloud Security Alliance (CSA). Top security concerns – CSA has identified top 7 cloud security threats. CSA has a draft document of cloud security controls.

5. Open questions and discussions

   a. Overall lexicon for CC, not limited to security is currently underway

   b. Connections of deliverables by NIST Cloud working groups. Develop documentation tree and outline relationship of various documents including version numbers

6. Security advantage in a CC environment
   a. Continuous of operation (leverage established infrastructure)
   b. Consistent service from existing assets
   c. Delegation of management overhead such as system updates, etc
   d. Small/medium agencies benefit from the scalability, and enhancement of security pasture comparing to lack of resource to keep up security measure
   e. Mouli: Virtual network segmentation as a security enabler vs. a threat
   f. Chris: Security enabler vs. threat depends on practical implementation and adoption

Chat transcript from room: cc_security
2011-02-09 GMT-08:00

[08:48] Jian Mao morphed into Jian Mao (NIST)

[09:58] anonymous morphed into Stacey Myers

[10:43] anonymous morphed into Harry J Foxwell (Oracle)

[10:51] anonymous morphed into Brian Ahier

[10:55] Jian Mao (NIST): working group page - http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

[10:55] anonymous morphed into James Denaro (Morrison)

[10:56] anonymous1 morphed into Nadeem Bukhari (Kinamik Data Integrity)

[10:57] anonymous morphed into Paul Hamman (Apptis)

[10:57] List of members: anonymous2, Brian Ahier, G. Hussain Chinoy (USDA NRCS), Harry J Foxwell (Oracle), James Denaro (Morrison), Jian Mao (NIST), John Molesky (DHS / DRC), Ken Stavinoha (Cisco), Mike McGee (Coalfire Systems), Nadeem Bukhari (Kinamik Data Integrity), Paul Hamman (Apptis)

[11:01] Jian Mao (NIST): web char room

[11:01] Jian Mao (NIST): http://webconf.soaphub.org/conf/room/cc_security

[11:01] anonymous morphed into Jon Truan (ORNL)

[11:01] Jian Mao (NIST): charter and meeting

[11:01] G. Hussain Chinoy (USDA NRCS): ramaswamy.chandramouli@nist.gov or mouli@nist.gov

[11:01] Jian Mao (NIST): mouli@nist.gov

[11:02] Jian Mao (NIST): charter and agenda at http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

[11:03] anonymous2 morphed into Jamal P. Le Blanc (Fujitsu)

[11:03] anonymous3 morphed into Joel Weise (Oracle)

[11:03] anonymous1 morphed into Jeremy Epstein (SRI International)

[11:04] Stacey Myers morphed into Stacey Myers (MITRE)

[11:04] anonymous morphed into R.K. Ferguson

[11:05] R.K. Ferguson morphed into R.K. Ferguson (Apptis)

[11:07] Harry J Foxwell (Oracle): Question: Some view cloud security as simply an extension of current distributed system security concepts and practices, while others view cloud security as something inherently more/different, especially concerning the use of virtualization. What is the view of this NIST working group?

[11:09] Jian Mao (NIST): "Analysis of Scope of Controls for Public Cloud Services" posted at the http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

[11:09] Jeremy Epstein (SRI International): +1 on that last comment about a threat taxonomy

[11:09] G. Hussain Chinoy (USDA NRCS): A taxonomy for threat modeling, in specific?

[11:11] Lee Badger (NIST)1 morphed into Lee Badger (NIST)

[11:12] Ken Stavinoha (Cisco): ISO Definition for IT Security: Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

[11:12] anonymous morphed into Gene Rackow

[11:14] anonymous morphed into Brad Gaylord

[11:14] Brad Gaylord morphed into Brad Gaylord (USDA NRCS)

[11:15] G. Hussain Chinoy (USDA NRCS): I guess that's the ontological model based on the taxonomy, Jeremy? (Sorry, being pedantic.)

[11:15] Jian Mao (NIST): is it a good idea to collect/develop a cloud specific security controls for US government on top of nist 800-53 and existing work done by groups such as CSA?

[11:16] G. Hussain Chinoy (USDA NRCS): +1 Jian Mao, absolutely. The CSA mapping would be a great contribution / start.

[11:16] Alan Sill (OGF): @Jian- I agree. Also our work here should be focused on cloud security standards development, not a broad effort at defining the topic in general

[11:16] Margaret Leary (Avaya Gov): GSA FedRAMP uses the 800-53 controls

[11:16] Jeremy Epstein (SRI International): I'm no expert on the lingo, so I'll pass on whether it's an ontological model on the taxonomy.

[11:17] Jian Mao (NIST): sounds like there is a need for assigning roles and responsibility for security controls to consumer and provider based on IAAS/PAAS/SAAS

[11:17] Alan Sill (OGF): Therea are several existing cloud security architectures, some customized to standards for particular service reference approaches, so one should not have the impression that a single set of standards will do.

[11:18] G. Hussain Chinoy (USDA NRCS): @Alan, agreed. That's part of the issue - providing guidance re: approaches + secarch.

[11:19] Lee Badger (NIST): alan, can you list the security architectures you are thinking about?

[11:19] Margaret Leary (Avaya Gov): I think there are existing efforts on GSA's part to define appropriate security controls applicable to cloud providers for U.S. government agencies. How will the standards we define complement those?

[11:20] Jian Mao (NIST): security control definition is in nist sp 800-53

[11:22] Alan Sill (OGF): Lee, these are being gathered in the RA group. In terms of standards, we can see WSRF-related approaches such as OGSA, GSI-based approaches such as used in Nimbus, and more generic ones such as used in OCCI, which relies on the underlying http(s) layer) and can work with any underlying authN//authZ model.

[11:22] G. Hussain Chinoy (USDA NRCS): I do think the RefArch/Tax WG can address taxonomic "views," including the related security taxonomy.

[11:23] Alan Sill (OGF): The Cloud Security Alliance (CSA) has an extensive categorization that will be presented at the RSA conference next week, which we might be able to get them to contribute.

[11:23] Lee Badger (NIST): alan, thanks.

[11:24] G. Hussain Chinoy (USDA NRCS): @Lee http://www.cloudsecurityalliance.org/cm.html

[11:25] List of members: Alan Sill (OGF), anonymous, Brad Gaylord (USDA NRCS), Brian Ahier, Ching Shih (ATT), Chris Braganza (MITRE), Chris Braganza (MITRE)1, Frederic de Vaulx (Prometheus Computing), G. Hussain Chinoy (USDA NRCS), Gene Rackow, Harry J Foxwell (Oracle), Jamal P. Le Blanc (Fujitsu),

James Denaro (Morrison), Jeremy Epstein (SRI International), Jian Mao (NIST), Joel Weise (Oracle), John Molesky (DHS / DRC), Jon Truan (ORNL), Ken Stavinoha (Cisco), Lee Badger (NIST), Margaret Leary (Avaya Gov), Matthew Chiodi (Deloitte), Mike McGee (Coalfire Systems), Nadeem Bukhari (Kinamik Data Integrity), Omar Fink (SAIC), Paul Hamman (Apptis), Paul Suh, R.K. Ferguson (Apptis), Stacey Myers (MITRE)1, Stu Martin
[11:26] anonymous morphed into E Brown (MITRE)
[11:27] Lee Badger (NIST): @Hussain, thanks for the link.
[11:28] G. Hussain Chinoy (USDA NRCS): np
[11:29] Alan Sill (OGF): v 1.4 coming out soon...
[11:29] Frederic de Vaulx (Prometheus Computing): We do want them to be addressed in the taxonomy working group
[11:30] Jian Mao (NIST): what should this working group to focus on and deliver vs reference architecture group and taxonomy group?
[11:32] Ken Stavinoha (Cisco): We should focus on the security expectations for various aspects of the cloud and who is reponsible for them
[11:32] G. Hussain Chinoy (USDA NRCS): @Jian, the mapping of various standards and maybe an interoperability framework? CSA does have a lot of great work on this.
[11:32] Alan Sill (OGF): Beyond architectures, we have to address concepts such as identity federation, standards for interchange of authorization and authentication credentials, federal use cases for identity management, NSTIC, DNSSEC, etc.
[11:33] G. Hussain Chinoy (USDA NRCS): That's a great point, @Alan, identity trust/interop is a big one.
[11:34] Jian Mao (NIST): @alan, sounds like an idea for top security concern requested by Mouli
[11:34] Alan Sill (OGF): Identity federations active in the academic research and federal cloud user space include the IGTF, InCommon (US-only), FedRAMP, etc. and should be recruited for their input.
[11:35] Ken Stavinoha (Cisco): My submission for the top 10 list is: Potential loss of control/ownership of data
[11:36] Alan Sill (OGF): Commercial providers such as Google, Yahoo, Verisign, and others that offer standards-compliant interfaces (e.g., via OpenID, OAuth, Shibboleth or other SAML-based methods, etc.) would also be good to include and get input for this group.
[11:37] Sundar Ramanathan (Capgemini): Data Integration , Privacy (PII) and Data Encryption cna be one of the top -10
[11:37] Jian Mao (NIST): in the US federal space, is A&A (or C&A) a big concern for systems or data being moved to the cloud?
[11:37] Mike McGee (Coalfire Systems): I think the CSA provides a decent list of top 7 that would be a good starting point
[11:37] G. Hussain Chinoy (USDA NRCS): @Alan, could you reiterate the identify federation issue for the top 10?
[11:37] Margaret Leary (Avaya Gov): A&A are concerns of GSA, who is setting up a JAB to oversee it
[11:38] Alan Sill (OGF): (To some degree, we are already gathering input in the http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory in terms of standards

applicable to security topics as well as other areas. Input is requested and welcome!)
[11:38] Harry J Foxwell (Oracle): top # concern: data remanance after deprovisioning
[11:38] G. Hussain Chinoy (USDA NRCS): @Jian Yes, that's a concern of the USDA, too; C&A for the cloud.
[11:38] G. Hussain Chinoy (USDA NRCS): (apologies for the doubling, not sure why that's happening)
[11:39] Frederic de Vaulx (Prometheus Computing): In which category would multi-tenant data/control separation be if any?
[11:39] Jian Mao (NIST): quote the speaker: what about a provider's compliance of the security req/policy of the cloud subscriber?
[11:39] Jeremy Epstein (SRI International): Top 10 submission: Ability to completely delete / destroy data when it may be replicated in unknown places.
[11:39] Margaret Leary (Avaya Gov): Yes - the ability for a provider to meet agency/customer-specific regulatory requirements (i.e. archival requirements)
[11:40] Jon Truan (ORNL): Certification and Accreditation requirements for Federal Clouds?
[11:40] Sundar Ramanathan (Capgemini): Open group Jericho forum is also a good reference - http://www.opengroup.org/jericho/publications.htm
[11:41] Jian Mao (NIST): Allan mentioned data privacy/data not leaving the country border
[11:41] Jeremy Epstein (SRI International): I know there's a lot of concern about data going offshore, but is it also reasonable to talk about data going from one state to another - since different states have different breach notification laws.
[11:41] Margaret Leary (Avaya Gov): Will U.S. Citizenship in data centers be an issue for agencies?
[11:42] R.K. Ferguson (Apptis): Doesn't much of the CSA work derive from Jericho ...?
[11:43] G. Hussain Chinoy (USDA NRCS): @Margaret FISMA compliance for cloud datacenters... isn't that a requirement that necessitates US citizenship?
[11:43] Sundar Ramanathan (Capgemini): The nuance around VM ecosystem /hypervisor Security in addition to IaaS/PaaS/SaaS security that deals with identity management, Authentication & Authorization needs to be considered as well
[11:44] Nadeem Bukhari (Kinamik Data Integrity): top 10 - Audit Data Integrity protection
[11:44] Alan Sill (OGF): A link to some useful talks on the topics being discussed:
http://indico.rnp.br/conferenceOtherViews.py?view=standard&confId=85 (Roundtable on Cloud and Grid Security Standards; 5th Anniversary IGTF and 12th TAGPMA Face-to-Face Meeting) Many useful talks by representatives of government agencies
[11:44] Margaret Leary (Avaya Gov): @ G. Hussain: It is, as I understand it.
[11:44] anonymous morphed into Thomas Porter (Digital Tool)
[11:45] Jian Mao (NIST): speaker mentioned audit for virtualization is very difficult
[11:45] G. Hussain Chinoy (USDA NRCS): FYI, top 7 threats from CSA

referenced:
http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[11:46] Ken Stavinoha (Cisco): Yes to make the list manageable and limit it to 10, we will need broad categories for these concerns
[11:46] Lee Badger (NIST): the NIST virt pub just went final
[11:46] G. Hussain Chinoy (USDA NRCS): Something like the OWASP Top 10
[11:48] Alan Sill (OGF): @Hussain, Mararet: Again, our focus should not be on determining policies such as citizenship requirements, etc., but on identifying the categories in which protocols, requirements and methods for automated communication and enforcement of these should exist.
[11:48] Jian Mao (NIST): lee asked for security advantage of cloud if there are any
[11:48] G. Hussain Chinoy (USDA NRCS): One benefit is having a regulated security behavior mediated by a contract (aka SLA).
[11:48] Sundar Ramanathan (Capgemini): In terms of vulnerability and threats OWASP is a good resource - http://www.owasp.org/index.php/Main_Page
[11:49] Margaret Leary (Avaya Gov): An advantage is that you have (hopefully) dedicated, trained resources - whereas many agencies don't have the resources in-house to effectively manage application security
[11:49] Alan Sill (OGF): @Jian: a benefit in practice is more professional administration of services, better coordination of response compared to individually maintained (and often not maintained) servers
[11:52] Lee Badger (NIST): in traditional networks, topology established perimeters to an extent; now with cloud it will be logical policies providing separation: which is better?
[11:52] R.K. Ferguson (Apptis): Should the threat taxonomy by incorporated into SP 800-144 ...
[11:54] Alan Sill (OGF): Passing on the following at the request of a colleague:
[11:54] Alan Sill (OGF): We have an initiative called SIF - Science Identity Federation - presently focused on US DOE national labs, user facilities, and projects - with the goal of bringing interoperable identity services to the DOE labs. You can see one of my slide decks here: http://bit.ly/gejzGv (this is from a DOE IT conference called NLIT, late May 2010) and you can join our group if interested http://groups.google.com/group/science-federation (this is a private, low volume mailing list to support SIF)
[11:54] Ken Stavinoha (Cisco): @Lee: Not sure that either is "better", but our antiquated US laws (like ECPA) more easily work with the concepts of boundaries and perimeters...
[11:55] Lee Badger (NIST): @Ken, agreed.
[11:55] Alan Sill (OGF): may I also mention the CILogon service we are contemplating using in the context of the SAJACC tests: http://cilogon.org
[11:56] List of members: Alan Sill (OGF), Brad Gaylord (USDA NRCS), Brian Ahier, Ching Shih (ATT), Chris Braganza (MITRE)1, E Brown (MITRE), Eugene Luster (R2AD), Frederic de Vaulx (Prometheus Computing), G. Hussain Chinoy (USDA NRCS), Gene Rackow, Harry J Foxwell (Oracle), Jamal P. Le Blanc (Fujitsu), James Denaro (Morrison), Jeremy Epstein (SRI International), Jian Mao (NIST), John Molesky (DHS / DRC), Jon Truan (ORNL), Ken Stavinoha (Cisco), Lee Badger (NIST), Matthew Chiodi (Deloitte), Nadeem Bukhari

(Kinamik Data Integrity), Omar Fink (SAIC), Paul Hamman (Apptis), Paul Suh, Stu Martin, Sundar Ramanathan (Capgemini), Thomas Porter (Digital Tool)
[11:56] Sent transcript to: maoj@knowceanconsulting.com
[11:56] Alan Sill (OGF): Thanks!